White paper
FUJITSU Security Solution SURIENT SCS (Stealth Connect Solution)

Durch die neue Stealth Connect Solution können sich berechtigte Anwender über ein sicheres Virtual Private Network (VPN) am Rechenzentrum anmelden. Für Angreifer ist das Rechenzentrum nicht ansprechbar und deshalb nicht angreifbar.

Inhalt

Einleitung

Mobilität und Konnektivität sind für einen erfolgreichen Geschäftsablauf von entscheidender Bedeutung. Manager reisen viel und tauschen jeden Tag sensible Daten über WLAN, integriertes UMTS oder jedes verfügbare Netzwerk aus. Daher gewinnt der Datenschutz stetig an Bedeutung. Haben Sie einmal darüber nachgedacht, was passieren könnte, wenn Ihre kritischen Geschäftsdaten in die falschen Hände geraten?

Der von Fujitsu im Forschungs- und Entwicklungsprojekt „Digitale Souveränität" entwickelte umfassende IT-Sicherheitsansatz geht über bestehende Konzepte weit hinaus: Für besonders schutzbedürftige Daten und Vorgänge bietet er eine bislang nicht erreichte Sicherheit – vom Endgerät über den Transportweg bis hin zum Rechenzentrum.
Die Entwickler und Ingenieure von Fujitsu haben dabei die möglichen Einfallstellen bei Endgeräten, beim Transportweg und im Rechenzentrum identifiziert und neuartige technische und organisatorische Maßnahmen konzipiert, um diese schließen zu können. Das Vorhaben „Digitale Souveränität" verfolgt die Zielsetzung, sichere Anwendungsumgebungen zu schaffen, die auf bestehenden und damit potenziell unsicheren Infrastrukturen aufsetzen, sowie ein Höchstmaß an Sicherheit zu gewährleisten – und das ohne Abstriche beim Bedienkomfort und bei der Performance.
Im Rahmen des Gesamtvorhabens „Digitale Souveränität" betrachtet Fujitsu vielfältige Einzelmaßnahmen und fügt diese zu einem schlüssigen Gesamtkonzept zusammen:

Die ersten verfügbaren Module sind:

- Managed Rack Solution (MRS) – Physischer Zugriffschutz für Server-Racks mit biometrischer Authentifizierung
- Sealed Rack Solution (SRS) – Hochsicheres Server Rack mit Schutz vor physischem Zugriff und elektronischen Angriffen
- Encrypted Boot Solution (EBS) – Automatisierter Bootvorgang von Servern mit verschlüsselten Festplatten
- Stealth Connect Solution (SCS) – Sichere VPN-Lösung für berechtigte Anwender
- Sealed Application Solution (SAS) – Ende-zu-Ende gesicherter Client mit verschlüsselter Kommunikation
- Secure Middleware Technology (SeMi) – Technologie für sichere Kommunikation zwischen Rechnern

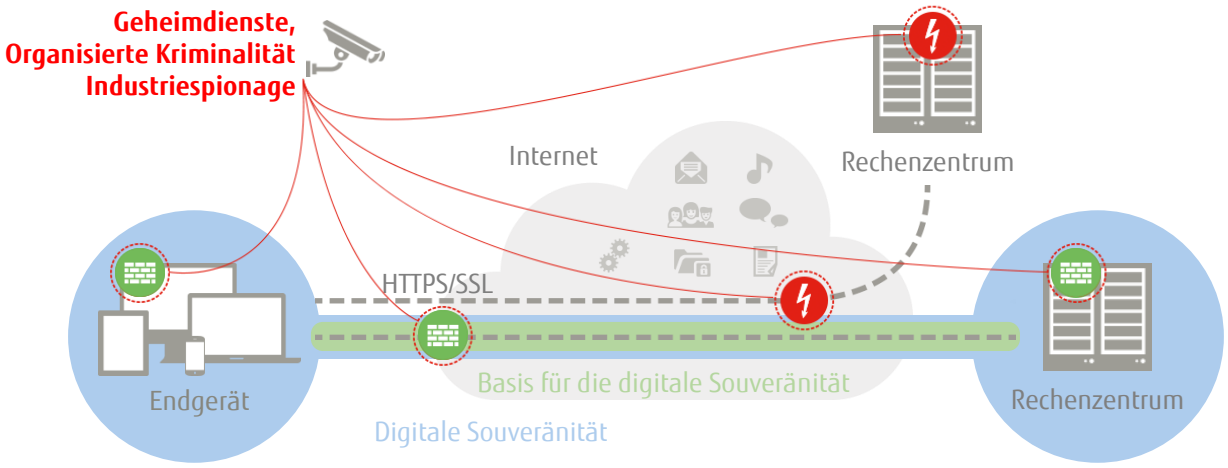

Abbildung 1: Durchgängige Sicherheit mit der Innovation „Digitale Souveränität" von Fujitsu

Im Folgenden wird die Stealth Connect Solution näher erläutert.

Zielsetzung

Ein externer Angreifer, der auf Daten des Rechenzentrums zugreifen will, beginnt meist mit dem „Abtasten" der Server mittels detaillierter Portscans, um mögliche Angriffspunkte zu finden. Wenn der Server (bzw. ein darauf laufender Dienst) auf die Anfragen antwortet, können Schwachstellen dieses Dienstes gefunden und ausgenutzt werden. Über diesen Weg kommen Angreifer normalerweise unerlaubt in die Systeme und können Daten abgreifen oder manipulieren. Autorisierte Anwender, für die eine Verbindung vorgesehen ist, können dagegen wie gewohnt eine Verbindung aufbauen – zum Beispiel zu einem Web-Service oder über ein Virtual Private Network. Beim Stealth Data Center ist jedoch der das VPN betreffende Port des Serverprozesses gesperrt und ein Angreifer erhält keine Antwort auf seine Portscans und somit auch keine Informationen darüber, wo überhaupt der Angriffspunkt zu finden wäre.

Die aktuelle Implementierung unterstützt den Aufbau von VPNs (Virtual Private Network) von beliebigen Standorten (wechselnde IP-Adressen) aus. VPNs ermöglichen den Aufbau einer sicheren, verschlüsselten Verbindung, über die beliebige andere Dienste eines Unternehmens genutzt werden können.

Für eine hohe Transparenz und Nachprüfbarkeit der Lösung sorgen u.a. die Verwendung von Open Source und die Offenlegung unserer Programm-Sourcen für unsere Kunden.

Basistechnologien
Folgend die wichtigsten Basistechnologien, die bei der Realisierung verwendet wurden:

- Als sicheres und gehärtetes Basisbetriebssystem für die Stealth Connect Solution wird die Linux-Distribution Debian eingesetzt.
- Als Basis für den sicheren Verbindungsaufbau der Stealth Connect Solution wird die Kommunikation der Secure Middleware über geschlossene Ports verwendet. Secure Middleware ist in einem separaten Whitepaper beschrieben.
- Aktuell ist der Aufbau eines VPN implementiert. Dieses unterstützt starke Verschlüsselung (konfigurierbar) sowie Perfect Forward Secrecy.
- Der Aufbau der VPN-Verbindung wird über ineinander geschachtelte Protokolle initiiert. Das Cracken eines der verwendeten Protokolle führt dabei nicht zu einer Freischaltung des VPNs. Dieses betrifft auch den Aufbau des VPNs selbst.

Derzeit werden die folgenden Methoden und Tools zur Verschlüsselung und Signatur verwendet bzw. unterstützt:

- OpenVPN
- GNU Privacy Guard (GnuPG)
- SSH

Komponenten der Lösung
Die Lösung setzt sich aus den folgenden Komponenten zusammen:

- Dezentrale Stealth Connect Box, die aus z. B. einem Office für alle PCs des Office ein spezifisches VPN zur Zentrale aufbaut. Alternativ wird künftig ein Windows-Software-Client (Stealth Connect Client) verfügbar sein (ggf. auf Kundenanforderung auch andere Betriebssysteme).
- Zentrale Stealth Connect Appliance, die das dahinterliegende Netzwerk der Zentrale gegen Angriffe schützt und eine vollständige Portsperre des VPN Servers gegen Angriffe aus dem Internet realisiert. Die Stealth Connect Appliance wiederum besteht aus einem internen Router, einem internen Relay-Server und dem eigentlichen VPN-Server.
- Definierte Vorgehensweise zur Integration in das Unternehmensnetzwerk
- Optionale Integration und Security Services

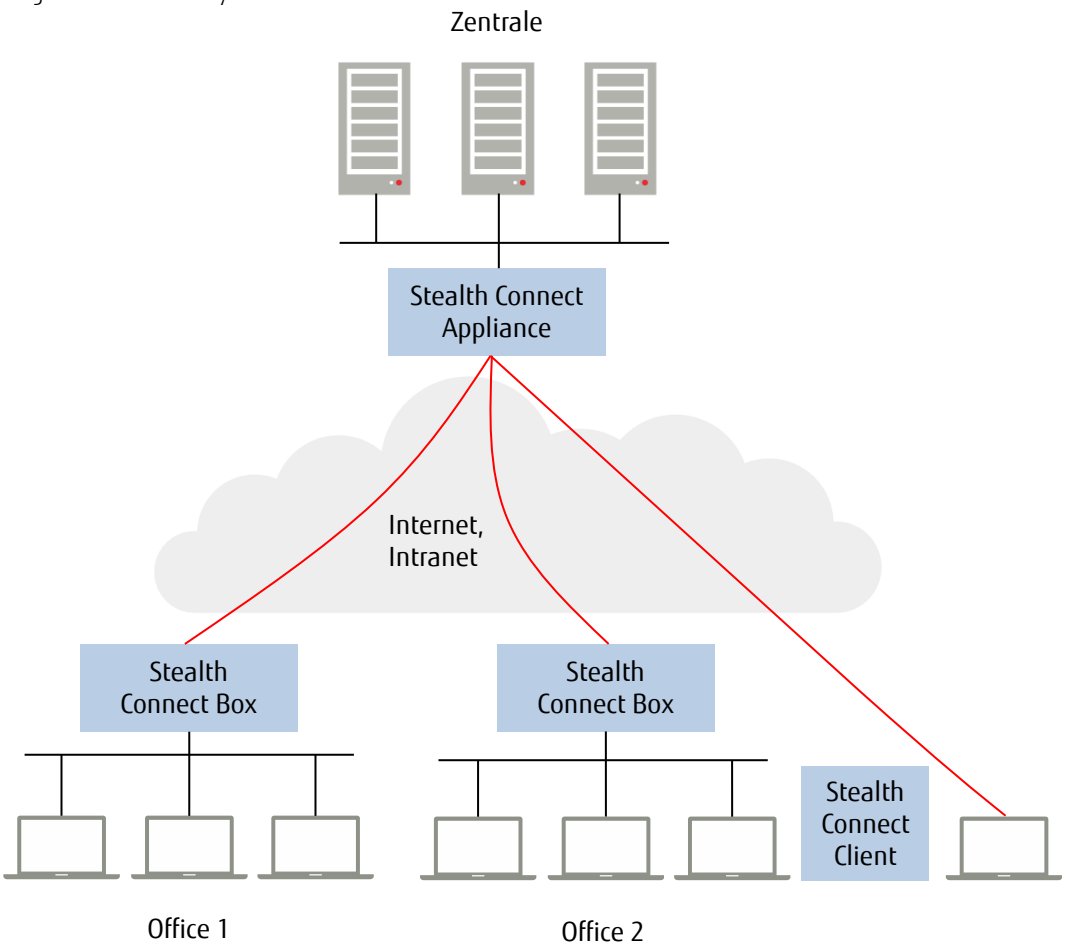

Abbildung 2: Komponenten der Lösung

Generelle Funktionsweise

Die Stealth Connect Solution sichert den Verbindungsaufbau einer dauerhaften Kommunikation (Session) ab. Hierbei wird verhindert, dass ein Angreifer irgendeinen verwendbaren Zugriff auf die Kommunikation erhält. Er wird vorher über einen Paketfilter abgeblockt – es existiert für ihn demzufolge kein offener Port, um einen Angriff auf das VPN zu versuchen. Dieses Ziel wird auch erreicht, wenn sich der Angreifer hinter demselben NAT befindet wie ein regulärer Anwender. Auch das Ausnutzen eines Zero Day Exploit [1] sowie Man-in-the-Middle Angriffe sind für einen Angreifer massiv erschwert.

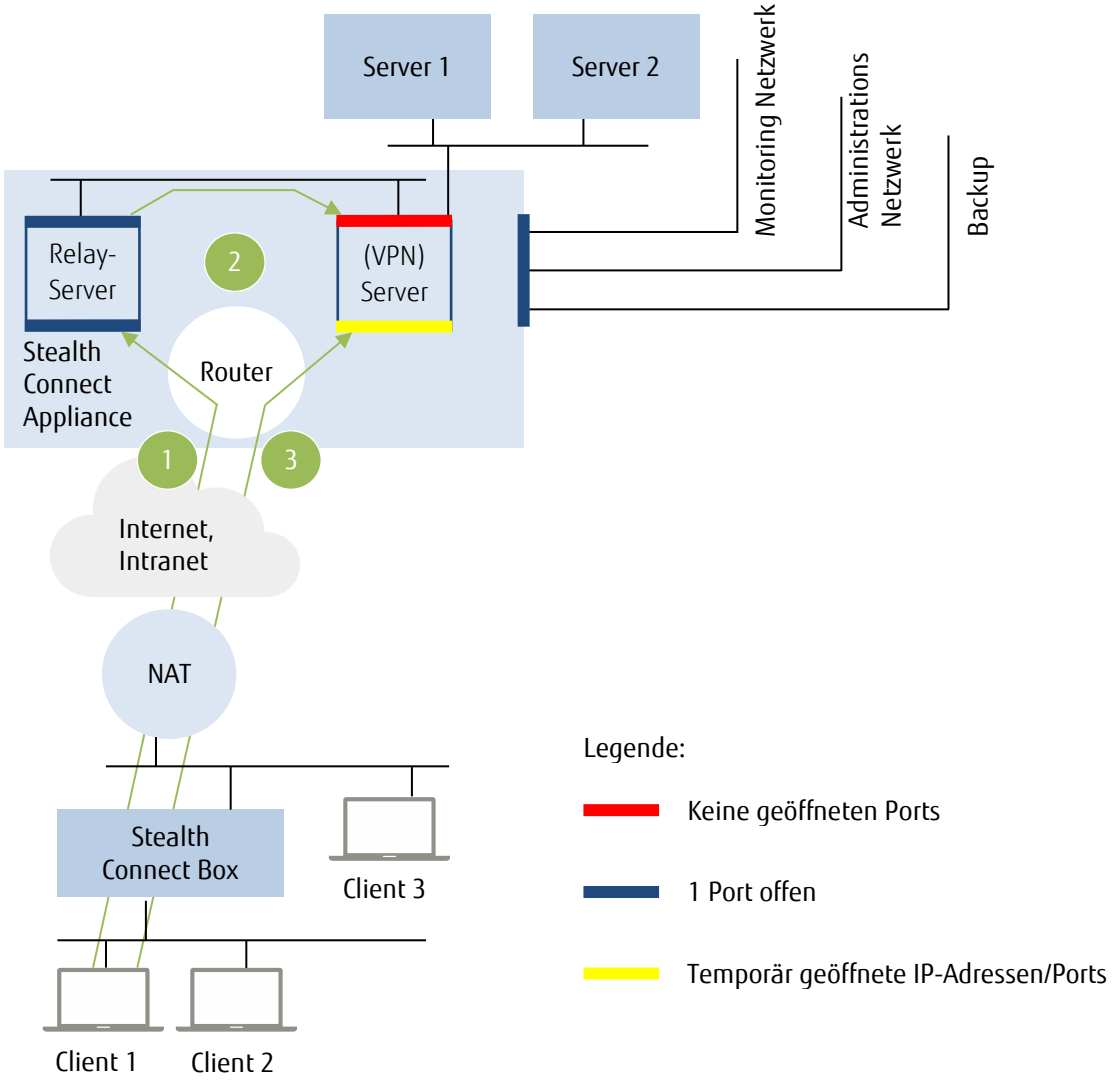

Abbildung 3: Generelle Funktionsweise der Stealth Connect Solution

Prinzipieller Ablauf:

1) Client1 sendet eine Anfrage zum VPN-Aufbau an die Stealth Connect Appliance. Die Stealth Connect Appliance empfängt diese Anfrage und verarbeitet sie intern. Dabei leitet sie die Daten intern an den Relay-Server weiter, der die Berechtigung hierfür überprüft. Der Relay-Server erzeugt eine zufällige Portnummer P und überträgt diese an Client1.
2) Der Relay-Sever sendet die vom Client erhaltenen Daten und Berechtigungen inklusive des zufälligen Ports P über die Secure Middleware an den VPN-Server. Auch in diesem Schritt werden die Berechtigungen wieder überprüft.
3) Client1 authentifiziert sich über den temporär für ihn geöffneten Port P am VPN-Server und baut das VPN auf. Anschließend wird die Kommunikationsbeziehung zu dieser IP-Adresse auf diesen spezifischen Client1 eingeschränkt. Andere, nicht authentisierte Clients hinter demselben NAT können so keine Verbindungsaufbauten mehr realisieren. Bestehende Verbindungen von authentisierten Clients werden davon nicht beeinträchtigt.

Client2 (z. B. in einer Büroumgebung oder Arbeitsgruppe) könnte ebenfalls über die Stealth Connect Box auf den VPN-Server zugreifen, während Client3 keinen Zugang zum Appliance-Server hat. Andere Clients, die nicht hinter dem gezeigten NAT platziert sind, erhalten während eines Anmeldeversuchs von z. B. Client1 keinerlei Informationen („offene Ports") vom VPN-Server.

[1] Zero-Day-Exploit nennt man einen Exploit, der eingesetzt wird, bevor es einen Patch als Gegenmaßnahme gibt. Die Entwickler hatten dadurch keine Zeit (zero day), die Software so zu verbessern, dass der Exploit unwirksam wird.

Hochverfügbarkeit

Kritische Komponenten wie die Stealth Connect Appliance können mit einfacher oder mehrfacher Redundanz ausgelegt werden. Die Stealth Connect Box kann im Bedarfsfall einfach durch eine identische Komponente ersetzt werden.

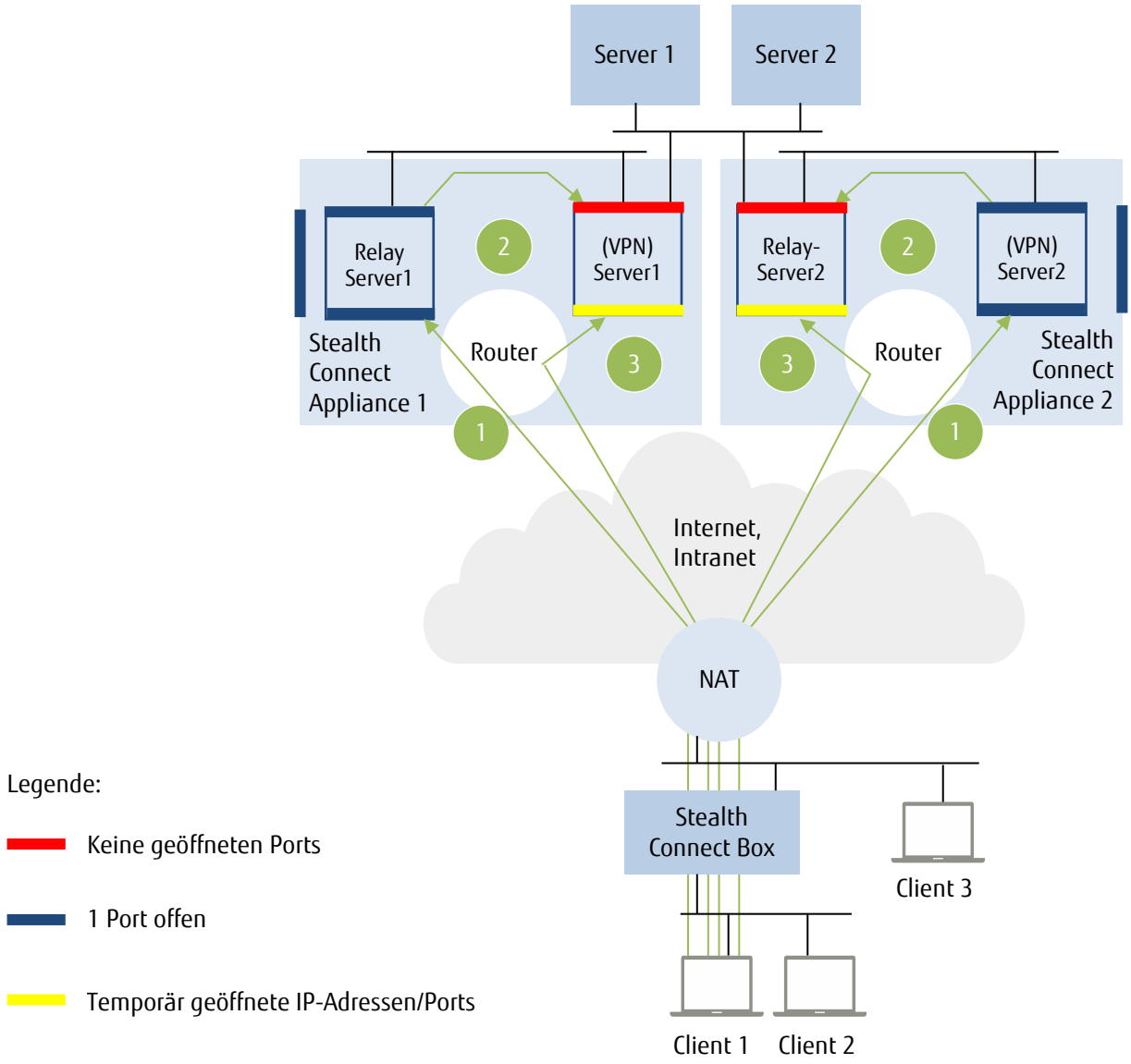

Abbildung 4: Redundanz mit zwei Stealth Connect Appliances

Prinzipieller Ablauf beim Verbindungsaufbau mit redundanter Stealth Connect Appliance:

- Client1 wählt zufällig einen der beiden Stealth Connect Appliances aus und versucht, das VPN aufzubauen.
- Falls dieser Verbindungsaufbau nicht möglich ist, wird der Vorgang an der anderen Stealth Connect Appliance wiederholt.

Kontakt
FUJITSU
Fujitsu Technology Solutions GmbH
Mies-van-der-Rohe-Strasse 8, 80807 München, Deutschland
Telefon: +49 1805 372-900*
E-Mail: cic@ts.fujitsu.com
Website: http://de.fujitsu.com
2012-04-01 CEMEA&I DE
* (Pro Anruf 14 Cent/Min.; die Preise für Anrufe aus dem Mobilfunknetz sind auf 42 Cent/Min. festgelegt worden)